March 2011

MONTHLY Cyber Security Newsletter

Security Tips

Mississippi Department of Information Technology Services

Division of Information Security

This issue…

This month's issue discusses ways to safeguard your personal data as well asa hot security topic in the social networking world.

Social Media Security

Your personal information can be accessible through a friend's social media page if you haven't restricted access in your account settings. Restrict third party's access to your information as well as unwanted users from seeing your information by tightening up your security settings.

Safeguarding Your Personal Data

Computers and the Internet have become an important part of our daily life, enabling a wide range of services to home users such as communicating with friends and family, shopping, paying bills, storing personal photos and music. This convenience and inter-connectivity does not come without risk however. Potential threats include viruses that could erase your entire system or hackers stealing your credit card information.

By understanding the risks and combining some common sense rules with a little bit of technology, home users can safeguard their data from these threats and understand the needs for security controls at work. The following tips will help protect your data.

Back Up Your Data

Your hard drive may crash or you may find that an infection has affected your computer so much that the operating system and applications need to be reinstalled. In cases like this it is best to have your important data backed up so you can restore your system without fear of losing your data. Below are some important steps you can follow:

- **Use your computer's backup tools.** Most operating systems provide backup software designed to make the process easier. External hard drives and online backup services are two popular vehicles for backing up files.
- **Back up data at regular intervals**. Weekly backups are recommended.
- **Verify the data has been backed up.** Backup media needs to be reviewed periodically to determine if all of the data has been backed up accurately.
- **Verify the ability to restore.** It is a best practice to periodically test that your backup data can be restored if loss occurs.

Use Strong Passwords

Passwords help protect your data. It is important to have a strong password for your computer, mobile device, and any other media used to store important and/or sensitive data. A strong password is at least eight characters that use a mix of upper case, lower case, and numeric or special characters. Each device should have its own strong password so that if one is compromised your others will stay secure.

Encryption

Encryption is a process whereby the data is scrambled and can only be read by someone with the "encryption key" to unscramble the data. Users should consider encrypting sensitive information. Some new operating systems include tools to encrypt data while others require the installation of encryption software.

Interesting Statistics…

Facebook demonstrates growth in total number of visitors, now over Yahoo in second place. Facebook has surged past Yahoo as the number two most popular site in the U.S.. As of July 2010, Facebook had crossed the 50 million user mark.

Be Safe Online

Below are a few helpful tips on how to keep safe on the Internet:

- Keep your operating system updated/patched. Set it to “auto update.”
- Use anti-virus and anti-spyware software and keep them updated
- Do not visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Secure your transactions. Look for the "lock" icon on the browser's status bar and be sure "https" appears in the website's address bar before making an online purchase. The "s" stands for "secure" and indicates that the communication with the webpage is encrypted.
- Keep your applications (programs) updated and patched, particularly if they work with your browser to run multi-media programs used for viewing videos. Set these programs to “auto update.”
- Block pop-up windows, some of which may be malicious and hide attacks. This may prevent malicious software from being downloaded to your computer.

Dispose of Information Properly

It is important to properly handle data erasure and disposal of electronic media (e.g. PCs, CDs, thumb drives) in order to protect confidential and sensitive data from accidental disclosure. Become familiar with the proper methods of sanitizing, destroying, or disposing of media containing sensitive information.

Before discarding your computer or portable storage devices, you need to be sure that data has been erased or "wiped." Below are a few tips to assist in disposing your data:

- Read/writable media (including your hard drive) should be "wiped" using Department of Defense (DOD) compliant software. Software that meets DOD compliance standards can be downloaded from the Internet at no cost.
- Shred CDs and DVDs. This type of media should be physically destroyed.
- Media that does not have a need to be re-used or contains sensitive or private data that cannot be "wiped" should be physically destroyed.

Resources For More Information:

- **US-CERT Tips for Safeguarding Your Data**
  - **http://www.us-cert.gov/cas/tips/ST06-008.html**
- **MS-ISAC Guidelines for Backing Up Information**
  - **http://www.msisac.org/awareness/**
- **MS-ISAC Newsletter – Backing Up Your Files**
  - **http://www.msisac.org/awareness/news/2010-02.cfm**
- **MS-ISAC Newsletter – Using Encryption to Protect Data**
  - **http://www.msisac.org/awareness/news/2008-05.cfm**
- **MS-ISAC Tip – Surf Safe On The Internet**
  - **http://www.msisac.org/daily-tips/Surf-Safe-on-the-Internet.cfm**
- **MS-ISAC Newsletter – Erasing Information and Disposal of Media**
  - **http://www.msisac.org/awareness/news/2006-08.cfm**

this newsletter is brought to you by…

MS-ISAC

www.msisac.org

www.its.ms.gov/services_security.shtml

An Increasing Threat Across Social Media Platforms: Third Party Applications

AliceClaire Thompson

It's a common misconception that social media applications are either created by the social network itself or, at the very least, are scanned for security vulnerabilities by the site managers prior to making them available to the public to use. According to Facebook's official statistics, people install 20 million applications every day and as of November 2010 there were approximately 550,000 active applications on the site. Facebook provides an API (Application Programming Interface) for developers to use to create applications that have the same look and feel of the social media platform. This look and feel provokes users to trust these applications because they look like they are a part of Facebook, however, these applications overall should never be completely trusted. You are responsible for all the information you provide on Facebook and most of these third party applications will have access to your profile and basic information even when you are not connected and using the application. Through the connection with the application, developers are able to use your personal information to target you more specifically with social engineering and phishing scams as well as potentially selling your information to other spammers who could potentially target you in a plethora of ways.

At the top of the scamming application list are applications that promise services that Facebook itself actually does not offer. BitDefener, an antivirus software suite, recently conducted a survey of 2, 700 users between the ages of 18 and 65 and in this survey it was found that the most popular scamming techniques were ones that offered some kind of stalking, such as letting you see who had viewed your profile, a feature that Facebook doesn't offer. Profile traffic insights or stalking applications accounted for 34.7% of the analyzed scams. BitDefender estimates that this type of scam has generated more the 1.4 million clickthroughs. Fake news articles or videos claiming "shocking images" were a mere click away accounted for 14.1%.

According to a report by ID Analytics released March 22, men on social networking sites were more likely than women to accept "friend" requests from members of the opposite sex, regardless of how well they know the requester. The same survey noted that on average, participants in the survey had 137 friends on a social network, but nearly 42% of those friends were people they did not actually know. It is estimated that 5% of adults in the United States will accept any friend request they receive, even if it comes from a stranger. This is important to note because by randomly accepting friend requests from users you do not know, you can be opening yourself and your network up to serious security breaches.

Things to remember when using social media:

1. If it sounds too good to be true, it probably is.
2. Just because an offer sounds legitimate and looks trustworthy, don't believe everything you see or read. The best practice is to always keep your guard up when using social media sites.
3. Most victims of internet crime act on impulse; use your head.
4. Unless you are sure of a person's identity, do not accept a friend request. Only accept requests from people you trust.
5. Always be cautious about sending sensitive information over the internet, especially if you are not confident in the security of the website.
6. Most phishing websites look identical to the legitimate site. Double check the URL prior to visiting any website published on a newsfeed.
7. Always be leery of emails requesting personal information from you or a colleague.